VIII kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 61)**

z dnia 8 czerwca 2017 r.

Pełny zapis przebiegu posiedzenia

Komisji Cyfryzacji, Nowoczesności i Nowoczesnych Technologii (nr 61)

8 czerwca 2017 r.

Komisja Cyfryzacji, Nowoczesności i Nowoczesnych Technologii, obradująca pod przewodnictwem posła **Pawła Arndta (PO)**, przewodniczącego Komisji, rozpatrzyła:

– informację Generalnego Inspektora Ochrony Danych Osobowych o zagrożeniach płynących z upowszechniania rozwiązań opartych na biometrii w kontaktach obywateli z instytucjami publicznymi i prywatnymi.

W posiedzeniu udział wzięli: **Marek Zagórski** sekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami, **Mariusz Cichomski** zastępca dyrektora Departamentu Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji wraz ze współpracownikami**, Ewelina Duda-Staworko** zastępca dyrektora Departamentu Spraw Obywatelskich Ministerstwa Spraw Wewnętrznych i Administracji wraz ze współpracownikami, **Agnieszka Bolesta** dyrektor Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji wraz ze współpracownikami, **Dariusz Ramocki** główny specjalista w Departamencie Bezpieczeństwa i Zarządzania Kryzysowego Ministerstwa Rozwoju wraz ze współpracownikami, **Wojciech Sawicki** dyrektor Departamentu Bezpieczeństwa i Ochrony Informacji Ministerstwa Finansów wraz ze współpracownikami, **Andrzej Kaczmarek** dyrektor Departamentu Informatyki w Biurze Generalnego Inspektora Ochrony Danych Osobowych, **Paweł Makowski** radca w Biurze Biurze Generalnego Inspektora Ochrony Danych Osobowych, **mł. insp**. **Radosław Jóźwiak** dyrektor Centralnego Laboratorium Kryminalistycznego Policji, **Mariusz Stolarz** doradca techniczny Najwyższej Izby Kontroli, **Joanna Karczewska** członek zarządu stowarzyszenia ISACA.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Ewa Gast i Julia Popławska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Paweł Arndt (PO):

Dzień dobry państwu. Otwieram posiedzenie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii. To już 61. posiedzenie w tej kadencji. Witam wszystkich przybyłych, witam państwa posłów i zaproszonych gości.

Porządek dzisiejszego posiedzenia to rozpatrzenie informacji Generalnego Inspektora Ochrony Danych Osobowych o zagrożeniach płynących z upowszechniania rozwiązań opartych na biometrii w kontaktach obywateli z instytucjami publicznymi i prywatnymi.

Powyższy porządek i materiały członkowie Komisji otrzymali. Czy są uwagi do porządku obrad? Nie ma uwag, stwierdzam zatem przyjęcie porządku. Przystępujemy do jego realizacji. Bardzo proszę pana Pawła Makowskiego, radcę w Biurze Generalnego Inspektora Ochrony Danych Osobowych, o przedstawienie informacji.

Radca w Biurze Generalnego Inspektora Ochrony Danych Osobowych Paweł Makowski:

Szanowny panie przewodniczący, szanowni panowie posłowie, panie ministrze i szanowni państwo, bardzo dziękujemy za możliwość przedstawienia informacji generalnego inspektora na temat bardzo ważnego zjawiska, jakim jest przetwarzanie danych biometrycznych. Pozwolę sobie na krótkie wprowadzenie, pokazujące, czym jest to zjawisko. Potem przekażę głos panu dyrektorowi Andrzejowi Kaczmarkowi, który szefuje działowi IT w Biurze GIODO.

Drodzy państwo, kiedy mielibyśmy jednym sformułowaniem opisać, jakie jest podejście głównego inspektora do używania biometrii i korzystania z nowych technologii w kontekście przetwarzania danych, to myślę, że warto użyć znanego wszystkim gdańszczanom stwierdzenia: *nec temere, nec timide*. I rzeczywiście zalecamy, by do nowych technologii w kontekście ochrony danych podchodzić bez zuchwałości, ale i bez lęku.

Naszą rolą jako Generalnego Inspektora jest dbanie o niezbędny balans pomiędzy podstawowym prawem określonym w art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej, tj. prawem do prywatności, a możliwością korzystania z nowoczesnych technologii. Często się mówi, że rola GIODO to rola hamulcowego. Tu pojawia się pytanie: czy chcielibyście państwo jeździć w samochodzie bez hamulców? Jakie konsekwencje i ryzyko mogłyby się z tym wiązać? To jest to *clou* rozważań na tema biometrii w kontekście ochrony danych. Chodzi o zaogrożenie, jakie może się wiązać z przetwarzaniem danych osobowych przy wykorzystaniu technologii biometrycznych. Niewątpliwie, co widzimy wszyscy, coraz częściej i chętniej do identyfikacji osób stosuje się systemy, które wykorzystują dane biometryczne. Od 2009 r. obywatele RP zostali wyposażeni chociażby w nowe paszporty biometryczne, a od marca 2015 r. w dowodach osobistych umieszczone są zdjęcia biometryczne. Tytułem przykładu w 2015 r. opiniowaliśmy tworzenie systemu informacji telefonicznej w biurach Krajowej Informacji Podatkowej. Zaopiniowaliśmy go negatywnie z uwagi na niespełnianie zasady adekwatności, brak wykazania niezbędności takich rozwiązań oraz brak podstawy prawnej. Chodziło o system weryfikacji głosowej podatników.

Dlaczego jest to tak ważne? Dane biometryczne stanowią szczególny typ danych osobowych. Są niezmienne. Kiedy porównamy je chociażby do najlepszego hasła, to hasło zawsze możemy zresetować, zmienić. Dane biometryczne są niepowtarzalne i ściśle związane z konkretną osobą. Są to informacje przynależące do osoby. Stanowią pewnego rodzaju identyfikator człowieka. Gdy dostaną się w ręce osób niepowołanych, może to skutkować kradzieżą tożsamości, o czym mówi się coraz częściej; prowadzi ona do poważnych i trudnych do odwrócenia konsekwencji. Zarówno pozyskiwanie, jak i udostępnianie danych biometrycznych powinno mieć miejsce tylko w wyjątkowych sytuacjach.

Rzeczywiście w wielu sytuacjach rozwiązania oparte na technologii biometrycznej są bezpieczne i użyteczne, co zauważamy i doceniamy. W opinii generalnego inspektora do wykorzystywania danych biometrycznych podchodzi się coraz powszechniej i niestety coraz bardziej bezrefleksyjnie; jedynie dla ułatwienia sobie życia, bez świadomości, że grozi to jednak stopniową utratą prywatności. Takie podejście zostało zaprezentowane w kilku opiniach grupy roboczej art. 29. Jest to zespół doradczy Komisji Europejskiej, w skład którego wchodzą rzecznicy ochrony danych osobowych z całej Unii Europejskiej. Mieliśmy kilka opinii, m.in. tę 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych czy 2/2012 w sprawie systemów rozpoznawiania twarzy w usługach online i usługach komórkowych.

Najbardziej problematyczne z perspektywy administratorów danych w kontekście biometrii jest to, że w obecnie funkcjonującym w Polsce systemie brak jest legalnej definicji danych biometrycznych. Możemy się posłużyć definicją, którą stworzono w ramach prac grupy roboczej art. 29 w opinii 4/2017. Możemy w niej przeczytać, że dane biometryczne to „właściwości biologiczne, cechy fizjologiczne, cechy życiowe lub powtarzalne czynności, przy czym te cechy i/lub czynności dotyczą danej osoby, a jednocześnie są wymierne, nawet jeżeli schematy używane w praktyce do ich pomiaru charakteryzuje pewien stopien prawdopodobieństwa”. Wobec braku ustawowych regulacji definiujących dane biometryczne, co jest poparte praktyką stosowania generalnego inspektora oraz znalazło odzwierciedlenie w kilku wyrokach Wojewódzkiego Sądu Administracyjnego, należy je traktować jako dane zwykłe, niepodlegające szczególnej ochronie. Niemniej w określonych przypadkach zestaw cech biometrycznych może oczywiście ujawniać dane wrażliwe, o czym mowa w artykule 27 ustawy.

W obecnym stanie prawnym dane biometryczne mogą być przetwarzane tak jak każde inne dane osobowe, kiedy istnieje ku temu podstawa prawna. Ustawa o ochronie danych osobowych wskazuje listę takich podstaw. One są wszystkie równoważne. Jest

nią zarówno zgoda na przetwarzanie danych, jak i przepis prawa. To są dwie główne podstawy wykorzytywane w sytuacji, kiedy przetwarzane są dane biometryczne. Pamiętać należy jednak o tym, że zawsze kiedy przetwarzamy dane, musimy wykazać spełnianie podstawowych zasad, jakie są właściwe dla systemu ochrony danych osobowych, np. tej, która mówi o proporcjonalności i minimalizacji danych. Chodzi o to, że zbieramy dane tylko w uzasadnionych sytuacjach, w którym bez ich wykorzystania niemożliwe byłoby osiągnięcie zamierzonego celu. Ponadto trzeba również spełnić zasadę, która mówi o tym, że dane trzeba należycie zabezpieczyć. Z naszej praktyki wynika to bardzo wyraźnie, bowiem inspektorzy biura kilkakrotnie w czasie czynności kontrolnych spotykali się z koniecznością oceny stosowanych przez podmioty publiczne i prywatne technologii biometrycznych, wykorzystujących chociażby odciski linii papilarnych palca, obrazy układu żył krwionośnych czy obraz tęczówki. Bardzo często nasze doświadczenia pokazywały, że dane były przetwarzane bez uzadnienia, bez podstawy prawnej albo gdy można było zrealizować cel, wykorzystując inny zestaw danych, nie tak bardzo ingerujących w prywatność.

Mamy trzy wyroki sądu, które możemy podać. Jeden z 2015 r. dotyczył przetwarzania danych biometrycznych przez jeden z klubów fitness. Do weryfikacji wchodzenia i wychodzenia do tego klubu zaczęto używać technologii biometrycznych w postaci skanu linii papilarnych. Zakwestionowaliśmy takie rozwiązanie. Finalnie administrator danych, a to dla nas również odzwierciedlenie wyroku sądu, zastosował alternatywną metodę sposobu weryfikacji. Kiedy mówimy o tym, że możemy zgodzić się na przetwarzanie danych biometrycznych w tym zakresie, to musimy mieć pewność, że zgoda jest dobrowolna. W tym wypadku uznaliśmy, że dobrowolność może zostać osiągnięta poprzez zastosowanie alternatywnej metody weryfikacji. Chodziło zatem o umożliwienie klientowi wejścia do siłowni wspomnianego centrum fitnessowego za pomocą innego indentyfikatora niż linie papilarne.

Innym przykładem są dwa wyroki z 2011 r., które dotyczą innej podstawy prawnej, czyli przepisu prawa. Są to dwie sprawy dotyczące sytuacji, w których administrator danych próbował przetwarzać dane biometryczne na podstawie art. 22^{1} Kodeksu pracy w celu weryfikacji czasu pracy pracownika. To wykorzystywanie również nie znalazło uzasadnienia, gdyż art. 22^{1} zawiera enumeratywną listę informacji, które można przetwarzać o pracownikach w celu chociażby weryfikacji czasu zatrudnienia. Tym samym stanowisko GIODO potwierdzone wyrokami WSA i NSA w jednym z przypadków zostało potwierdzone i uznaliśmy brak możliwości przetwarzania danych biometrycznych w tym zakresie.

Zanim przekażę głos panu dyrektorowi Kaczmarkowi, powiem, że to, co teraz jest punktem odniesienia dla wszystkich, którzy zajmują się ochroną danych osobowych, to ogólne rozporządzenie o ochronie danych. Akt wypracowany przez instytucje unijne, który wszedł w życie 24 maja 2016 r., będziemy stosować od 25 maja 2018 r. Na szczęście w ogólnym rozporządzeniu mamy już wyraźnie zdefiniowane dane biometryczne, ale co najważniejsze – dane biometryczne zostały uznane za dane wrażliwe, wymagające szczególnej ochrony.

Przepisy rozporządzenia przewidują kilka sytuacji, w których dane wrażliwe, dane szczególnej kategorii, bo taka jest definicja legalna, mogą być przetwarzane. Może to być wtedy, kiedy osoba, której dotyczą, wyrazi na to wyraźną zgodę albo kiedy przepis prawa umożliwia przetwarzanie takich danych. Bardzo się cieszę, że na sali są przedstawiciele Ministerstwa Cyfryzacji z panem ministrem na czele, gdyż Ministerstwo Cyfryzacji jest odpowiedzialne za wdrożenie polskich przepisów o ochronie danych osobowych, które umożliwią pełne stosowanie rozporządzenia. Jednym z elementów prac jest nowelizacja przepisów sektorowych. Rozporządzenie wprost dopuszcza możliwość przetwarzania danych biometrycznych, chociażby w systemach ochrony zdrowia, o ile przepis prawa państwa członkowskiego taką możliwość dopuszcza.To samo dotyczy wspomnianego już art. 22^{1} Kodeksu pracy. Jest dość duża dyskusja publiczna w tym zakresie. Wiele podmiotów domaga się możliwości przetwarzania danych biometrycznych w stosunkach pracy. I tu jest duża rola ministra cyfryzacji, żeby na etapie nowelizacji sektorowych skoordynować prace wszędzie tam, gdzie będzie to niezbędne. Chodzi o test niezbędno-

ści dla demokratycznego państwa prawnego w sytuacji, w której będziemy umożliwiać przetwarzanie osobowych danych biometrycznych, chociażby w kontekście zatrudnienia. Czekamy na wyniki działań legislacyjnych w tym zakresie.

Drodzy państwo, ze swojej strony bardzo serdecznie dziękuję. Przekazuję głos panu dyrektorowi Kaczmarkowi, który przygotował dla państwa kilka bardzo ciekawych slajdów, dotyczących technicznych aspektów przetwarzania danych biometrycznych i ryzyka zagrożeń, które wiążą się z tym procesem. Bardzo proszę, panie dyrektorze.

Dyrektor Departamentu Informatyki w Biurze Generalnego Inspektora Ochrony Danych Osobowych Andrzej Kaczmarek:

Szanowny panie przewodniczący, szanowni państwo, na swoim slajdzie chciałbym przedstawić elementy, które będą istotne w momencie, kiedy będziemy mieli podjąć decyzję. Samo powiedzenie, że używamy danych i technik biometrycznych, nie oznacza wiele. Mamy bowiem różne techniki biometryczne, różne źródła tych technik, różne zagrożenia i różne sytuacje.

Chciałbym krótko przedstawić pewne aspekty związane z tym zagadnieniem. Nie będę pokazywał już slajdów dotyczących definicji danych biometrycznych zawartych w RODO, ale również w normach, które także potwierdzają ten kierunek podejścia, że dane biometryczne uważamy w tym zakresie, który dotyczy zautomatyzowanego przetwarzania danych. Chodzi o to, żeby nie mylić ich z danymi biometrycznymi, takimi jak zdjęcie zamieszczone w CV albo odręczny podpis pracownika, który stanowi dane biometryczne z punktu widzenia pierwotnej definicji przyjętej przez grupę art. 29. Dlatego zajmiemy się tylko aspektami przetwarzania technicznego związanego z automatycznym przetwarzaniem i użyciem wzorca, pewnego schematu przetwarzania.

Musimy sobie zdawać sprawę, że w przypadku danych biometrycznych zawsze musimy mieć jakieś ich źródło. Owym źródłem mogą być różne elementy: odcisk palca, sposób mówienia, czyli tzw. dane behawioralne. Jeśli chodzi o wzorzec, to poddając się weryfikacji, oddajemy dane surowe. Dane w stanie surowym muszą być przetworzone do postaci, w której są potem porównywane z wzorcem odniesienia, który musi zostać wprowadzony do systemu informatycznego w momencie rejestracji użytkownika. W związku z tym mówimy o tzw. danych surowych i danych przetworzonych, które stanowią odpowiedni wzorzec dopasowania. Przetwarzanie odbywa się na etapie pobierania źródła, czyli przytknięcia palca do odpowiedniego urządzenia czy też spojrzenia w kamerę, która wykonuje obraz naszej twarzy.

Wiadomo, że użycie danych do identyfikacji wymaga od cech stanowienia pewnych właściwości. Istotne właściwości, które są brane pod uwagę, to: uniwersalność, czyli na ile ten typ danych jest w posiadaniu każdego osobnika; unikalność, czyli jak unikalnie definiują daną osobę; stałość i niezmienność w czasie, bo pewne dane ulegają zmianie w czasie, np. niektóre dane biometryczne w stosunku do dzieci muszą być odnawiane – co rok do 16 roku życia, dopiero potem pozostają niezmienne. Dalej jest łatwość pobrania. Inna jest łatwość pobrania odcisku palca, a inna jest sytuacja w przypadku, kiedy pobieramy kod DNA. Kolejną kwestią jest akceptowalność, czyli to, na ile dane nie budzą wątpliwości co do ich pobierania ze strony użytkownika. Chodzi o brak negatywnych skojarzeń. Wiadomo, że odcisk palca kojarzony jest z metodami policyjnymi, dochodzeniowymi. Pobranie danych w postaci siatkówki oka rodzi zagrożenie zdrowia. Kolejna cecha to łatwość obejścia, czyli to, na ile użyta technologia jest możliwa do podrobienia, na ile można oszukać system. Jest wiele konkretnych przypadków oszukania systemu biometrycznego, zatem nie zawsze ten system jest dokładniejszy.

Tak jak już powiedziałem, system biometryczny działa w ten sposób, że najpierw rejestruje się dane użytkownika, owy wzorzec odniesienia, a potem następuje pobranie wzorca przy każdym przypadku weryfikacji. Pierwszym przypadkiem jest punkt rejestracji, w którym identyfikuje się użytkownika, sprawdza się i zapisuje w bazie danych jego tożsamość z danymi biometrycznymi. Przy czym rozwiązania te są różne. W zależności od tego, jaka jest architektura systemu, możemy różnie mówić o bezpieczeństwie danych. Są takie przypadki, że mamy centralną bazę użytkowników i ich danych biometrycznych, np. bank stosuje taką bazę, a są przypadki, gdzie dane biometryczne

z danymi identyfikującymi są zapisywane na karcie i wręczane osobie, której dotyczą. Identyfikacja polega na tym, że w momencie przejścia przez bramkę osoba podstawia kartę i zostawia swój odcisk palca. Dane nie są zapisane nigdzie indziej niż karta, którą ma w posiadaniu użytkownik i to właściwie wszystko. To jest ważne z punktu widzenia bezpieczeństwa.

Ważnym elementem jest tak zwany wskaźnik błędnej akceptacji, wskaźnik błędnych odrzuceń, czyli to, na ile dany system biometryczny jednoznacznie identyfikuje osobę. Mamy tutaj do czynienia z bardzo szerokim przedziałem. Począwszy od wskaźnika równego 10 aż do wskaźnika 0,0001. W tym ostatnim przypadku mamy bardzo dużą dokładność identyfikacji. Wskaźnik błędnej akceptacji jest bardzo istotny, ale równie istotny jest wskaźnik błędnych odrzuceń, dotyczący sytuacji błędnego rozpoznania osoby poddającej się identyfikacji. System w każdym przypadku – zarówno w momencie rejestracji, jak i weryfikacji – za każdym razem pobiera rzeczywisty obraz, surową próbkę. Próbka może być inna, gdyż możemy bardziej docisnąć palec albo będzie on mocniej przekrzywiony; układ twarzy może być inny. Dlatego właśnie trzeba brać pod uwagę techniczne aspekty realizacji konkretnego systemu. Istotne są takie takie elementy, jak: akceptowalność, łatwość użycia, czas rejestracji, czyli to, ile czasu potrzeba na zarejestrowanie osoby w bazie danych oraz na identyfikację i weryfikację w przypadku rzeczywistego wykorzystania danych. Kolejne elementy to wiarygodność i miara zaufania, głównie współczynniki błędnej akceptacji i błędnego odrzucenia, oraz wielkość wzorca, która ma wpływ na takie elementy techniczne jak wielkość bazy danych.

Podsumowanie parametrów takich jak akceptowalność, łatwość użycia, czas weryfikacji domaga się oceny, co jest najbardziej i najmniej korzystne z punktu widzenia użytkownika. Najmniej wątpliwości pod względem akceptowalności budzą głos, rysy twarzy, układ krwionośny palca, linie papilarne. Natomiast pewne wątpliwości budzą odręczny podpis i siatkówka. Pod kątem łatwości użycia: głos i rysy twarzy oraz tęczówka i siatkówka, które wymagą odpowiedniego zbliżenia i ustawienia w stosunku do kamery, podczas gdy do kształtu twarzy wystarczy, że jesteśmy w polu widzenia kamery. Elementy te są istotne z punktu widzenia wygody i jakości danego systemu biometrycznego.

Przejdę do zagrożeń, bo o tym głównie będziemy mówić. Można wyróżnić 8 kategorii zagrożeń. Pierwszym jest możliwość ujawnienia danych wrażliwych. W przypadku takich danych źródłowych jak np. oko czy twarz, na podstawie rysów twarzy można zidentyfikować narodowość czy grupę etniczną. Na podstawie oka – stan zdrowia, bycie pod wpływem alkoholu; te elementy mogą zostać ujawnione na podstawie tego właśnie źródła danych biometrycznych. Kolejnym zagrożeniem są ograniczone możliwości zmiany i unieważnienia wzorca. Jak już zostało powiedziane w kontekście danych źródłowych, nie jesteśmy w stanie ich zrobić ani zmienić. Jedynie przeszczep skóry czy innych elementów może spowodować zmianę danych biometrycznych. Są jednak techniki biometryczne, które umożliwiają tworzenie odnawialnych źródeł danych biometrycznych, odnawialnych wzorców danych biometrycznych. Chodzi o tworzenie wzorca na podstawie danych źródłowych plus na podstawie innych danych, np. podpisu czy numeru PIN, tak zniekształcanych, że stworzą unikalny wzorzec z tych dwóch elementów. Jeżeli poprzedni wzorzec został skompromitowany, to zmieniając możliwy do zmiany element, możemy utworzyć nowy wzorzec danych biometrycznych.

Innym zagrożeniem jest możliwość użycia danych bez wiedzy osoby, której dane dotyczą. Wiadomo, że jeśli chodzi o układ żył krwionośnych palca lub dłoni, to trudno pobrać takie dane bez wiedzy użytkownika, ale takie dane jak kształt twarzy czy elementy związane z siatkówką oka mogą być pobrane i wykorzystane bez wiedzy użytkownika, którego dotyczą. Kolejnym zagrożeniem jest trudność pobrania próbki biometrycznej. Jedne próbki są łatwe do pobrania, inne z kolei wymagają pewnej troski osoby poddawanej weryfikacji, np. pobranie linii papilarnych z wytartych pracą lub skaleczonych palców może być trudne. Odnosi się do określonej grupy osób, takich jak pracownicy budowlani oraz pracownicy innych zawodów powodujących wytarcie palców. Chodzi też o odpowiednie użycie właściwych źródeł danych biometrycznych.

Następnym zagrożeniem jest podatność na łączenie danych. Drodzy państwo, jeżeli bazujemy na czynniku identyfikującym jako wzorcu odniesienia danych biometrycznych,

to, mając w posiadaniu dwa różne zbiory danych, możemy je połączyć poprzez identyfikator, wiedząc, że dane dotyczą jednej osoby, i uzyskać nową jakość danych, określony profil właściciela danych. Kolejne zagrożenie to brak przejrzystości. Zasady działania większości systemów biometrycznych objęte są tajemnicą producenta. Nie przekazują oni informacji, w jaki sposób tworzony jest wzorzec, w jaki sposób wykonywane jest porównanie. Dają tylko te parametry, które są istotne dla odbiorcy jako użytkownika, czyli współczynnik FAR, tj. współczynnik błędnej akceptacji i błędnego odrzucenia. One punktu widzenia eksploatacyjnego są najważniejsze.

Kolejnym zagrożeniem jest możliwość błędnej identyfikacji, weryfikacj i klasyfikacji. Mówi ono o tym, że technologia biometryczna identyfikacji bazuje na porównywaniu wyekstrahowanych cech biometrycznych pobranej próbki z wyciągniętymi w taki sam sposób cechami biometrycznymi próbki wzorca. Stąd różnica pobranych próbek może być spowodowana tym, że w inny sposób przyłożymy palec czy inaczej ustawimy się w momencie pobierania owego wzorca, w momencie identyfikacji.

Dalej jest możliwość fałszerstwa. Pokazanych było wiele sytuacji udowadniających, że proces identyfikacji i weryfikacji można oszukać. Wykonywane było np. pobranie odcisków palca ze szklanki czy lustra, odpowiednie wzmocnienie ich poprzez użycie jakichś proszków; zrobienie i przyłożenie zdjęcia. Jeżeli czujnik reagował także na temperaturę i inne dane, to odpowiednie użycie odcisku lateksowego czy z ciastoliny umożliwiało oszukanie systemu.

Ostatnie doniesienie dotyczące telefonu samsung s7, gdzie weryfikacja opierała się na tęczówce oka pokazało, że system został złamany. Wystarczy podłożyć zdjęcie wykonane na drukarce i nałożyć na oczy odpowiednie szkła kontaktowe, które powodują, że system rozpoznaje atrapę jako rzeczywistą osobę. Elementy fałszerstwa istnieją, chociaż w wielu przypadkach można pokazać, że systemy działają z dużą dokładnością, w przypadku chociażby układu żył krwionośnych czy *palm secure*, czyli układu żył krwionośnych dłoni – technologii opracowanej przez firmę Fujitsu.

Proces składa się z dwóch etapów, które tutaj pokazałem. Pierwszym jest preparowanie próbki, a drugim jej użycie. Widzimy, że nie są to w 100% bezpieczne metody, natomiast w wielu przypadkach są bardziej dokładne i potrafią wyróżnić więcej cech niż potrafi osoba, która ocenia osobę. Wyobraźmy sobie, że mamy zdjęcie w dowodzie i osobę, która posługuje się dowodem. Mogą być one na tyle podobne, że nie do rozróżnienia dla osoby, która porównuje zdjęcia. Nie wie ona, czy jest to falsyfikat; czy to jest ta osoba, czy inna. Natomiast system biometryczny, który bazuje na punktach charakterystycznych twarzy, takich jak odległość oczu, odległość oczu od nosa, proporcje tych odległości czy skrajne punkty, jest w stanie na podstawie tych danych dokonać rozróżnienia. I to pomimo że osoba jest odpowiednio ucharakteryzowana, zmieniła fryzurę, ma wąsy itd. Tak więc w niektórych przypadkach system biometryczny jest bardziej dokładny i nie można go przekładać na tę stronę czy na tę stronę. Zawsze należy wziąć pod uwagę wszystkie aspekty związane z kontekstem, w jakim dane zostaną użyte.

To, co powiedziałem, dotyczyło zagrożeń. Teraz opowiem o tym, jakie są zalety. Należy do nich brak możliwości dzielenia się danymi biometrycznymi z inną osobą. Jeżeli posługujemy się danymi biometrycznymi, to nie możemy ich przekazać innej osobie. Natomiast kartę wejścia do danego pomieszczenia już tak, co było często wykorzystywane np. przez lekarzy w szpitalach. Można ją przekazać innej osobie, zmienić termin wyjścia z pracy czy wejścia do pracy. W przypadku danych biometrycznych tego nie zmienimy, nie pożyczymy, nie przekażemy danych innej osobie.

Kolejną zaletą jest brak możliwości zapomnienia danych. Hasło możemy zapomnieć, kartę możemy zostawić w innym garniturze, natomiast danych biometrycznych nie zapomnimy, bo są one tam, gdzie my jesteśmy.

Zaletą danych biometrycznych jest też odporność na ataki fałszerstwa dla niektórych metod. Dla niektórych metod możliwości fałszerstwa są bardzo małe,wręcz minimalne, natomiast dla niektórych bardzo duże w zależności od konkretnego systemu biometrycznego.

Dalej mamy wiarygodność, która jest związana z możliwością ataku fałszerstwa, ze źródłem danych biometrycznych, ale również z jakością samego systemu. Na kolejnych slajdach króciutko wymienię systemy biometryczne, takie jak biometria linii papi-

larnych, i wskażę elementy, które są słabymi punktami i zaletami danego systemu. Wiadomo, że w przypadku linii papilarnych tym słabym punktem jest możliwość użycia bez wiedzy właściciela z uwagi na pobranie chociażby ze szklanki czy w jakiś inny sposób. Łatwość podrobienia jest dość duża. Brak możliwości wymiany, dzielenia się, brak możliwości zapomnienia – to jest oczywiste, że to istnieje. Przeważające są negatywne cechy, czyli łatwa możliwość podrobienia. W przypadku układu żył dłoni też mamy możliwość użycia bez wiedzy właściciela, ale jest bardzo mała. Taka możliwość jest w przypadku, kiedy osoba jest nieświadoma, ale musi żyć. Był taki przypadek w jednym ze szpitali amerykańskich, że osobę, którą przywieziono do szpitala, mimo że ta nie była świadoma, zidentyfikowano podstawie kształtu żył dłoni, bo już wcześniej była zarejestrowana w tym szpitalu.

Kolejną kwestią jest bardzo duża trudność podrobienia próbki biometrycznej, ponieważ badany jest element przepływu krwi, żywotności obiektu. Możliwość fałszerstwa czy błędnej identyfikacji praktycznie nie istnieje, a przynajmniej jest bardzo mała. A to dlatego, że współczynnik FAR wynosi 0,0001, czyli 1:100 000 000 czy 1:10 000 000, nie pamiętam; jest to wyrażone w procentach. Brak możliwości wymiany, dzielenia się danymi, duża odporność na fałszerstwa – to są zalety. Mamy też układ twarzy, w przypadku którego zaletą jest łatwość pobrania tego wzorca. Jednocześnie jest to też zagrożenie, bo można pobrać te dane bez wiedzy użytkownika, którego owe dane dotyczą. Jedna cecha jest więc zaletą, a druga wadą. Trudność pobrania próbki biometrycznej praktycznie nie istnieje, bo wystarczy odpowiednia jakość kamery i mamy pobranie danych bez wiedzy użytkownika.

Dalej mamy ograniczoną możliwość zmiany i unieważnienia. Tu są ograniczone możliwości, dlatego że w większości systemów biometrycznych istnieją techniki, nie wszyscy je stosują, które dają możliwości odnowienia wzorca, czyli łączenia z dodatkowym elementem.

Elementy prawne były już omawiane, więc nie będę wskazywał konkretnych punktów czy też ustaw i rozporządzeń, które mówią o legalności przetwarzania. Mam zestawienie odnośnie do kontroli, które były przeprowadzane. Było ich kilka. W wielu przypadkach, zwłaszcza tam, gdzie to wynikało z przepisów prawa, nie było zastrzeżeń. W wielu przypadkach dotyczących przetwarzania danych pracowników zostały wydane negatywne decyzje. Zostały one poparte wyrokami sądu, mówiącymi o tym, że przetwarzanie danych jest niemożliwe w określonej sytuacji prawnej, dlatego że mamy takie, a nie inne przepisy prawa, które odpowiednio nakładają się na siebie.

Przejdę do wymagań dotyczących bezpieczeństwa. tj. poufności, integralności, odnawialności i unieważnienia. Są to elementy, które trzeba brać pod uwagę przy ocenie danego systemu. Chodzi o to, na ile w danym systemie dane biometryczne są chronione, czy w ogóle istnieje potrzeba ich przetwarzania przez administratora danych, czy mogą być przetwarzane przez osobę, której dane dotyczą, niegromadzone w centralnej bazie danych. Integralność danych, odnawialność, unieważnienie – chodzi o to, na ile dana technologia pozwala na stosowanie technik takich jak *renewability*, czyli odnawialność danych biometrycznych.

Jeśli chodzi o nieodwracalność, to wiadomo, że dane, które są przetwarzane, są z reguły nieodwracalne. Wzorzec stworzony w wyniku matematycznego przetworzenia danych źródłowych stworzony jest za pomocą funkcji jednokierunkowej. Nie da się z tego wzorca odtworzyć danych surowych w innym systemie.

Dalej mamy dyskretność zabezpieczeń wzorca odniesienia przed nieautoryzowanym pobraniem jego wartości. Te elementy musimy brać pod uwagę przy ocenie architektury i bezpieczeństwa systemu informatycznego, który wykorzystuje owe dane.

Jeśli chodzi o użycie danych biometrycznych w nowym systemie prawnym, czyli w momencie wejścia w życie RODO, musimy wziąć pod uwagę to, że użycie danych warunkuje przepis prawa lub inne elementy, takie jak podana przeze mnie wcześniej zgoda użytkownika. Trzeba rozważać także elementy ogólne, takie jak proporcjonalność.

RODO zawiera taki element jak ocena skutków ochrony danych osobowych. Podsumowując, różne doświadczenia i metody, można powiedzieć, że nie można wydać wyroku, czy dana technologia jest dobra, właściwa i można ją stosować. Musimy wziąć pod uwagę

aktualny stan prawny, wymagania przepisów, tj. czy przepis zezwala. W przypadku zgody, trzeba brać pod uwagę także to, czy spełnione są inne warunki, takie jak dobrowolność zgody, adekwatność i proporcjonalność danych w stosunku do celu, któremu mają służyć. A to dlatego, że inna jest sytuacja, kiedy nastąpi atak i np. niewłaściwa osoba wejdzie do siłowni i z niej skorzysta, a inna, jeżeli system zostanie oszukany w przypadku wejścia do systemu bankowego i pobrania pieniędzy z konta danej osoby. Trzeba brać pod uwagę zagrożenia, kontekst i wszystkie elementy. Dlatego właśnie w grę wchodzi ocena skutków dla ochrony prywatności, którą w każdym przypadku danych biometrycznych należy przeprowadzać z uwagi na to, że dane te należy zaliczyć do kategorii danych szczególnie chronionych. Trzeba wziąć pod uwagę elementy związane z kontekstem, bezpieczeństwem oraz wszystkie zagrożenia i to z punktu widzenia zarówno administratora danych, jak i osoby, która z nich korzysta.

Podsumowując, chciałbym zwrócić uwagę na elementy, które wynikają z tego wszystkiego. Mianowicie wydawanie środków identyfikacji biometrycznej jest uzasadnione wtedy, kiedy stanowi o tym przepis prawa, np. wydawanie środków identyfikacji biometrycznej, dla których rozporządzenie wymaga zapewnienia wysokiego poziomu bezpieczeństwa. W rozporządzeniu wykonawczym Komisji powiedziane jest wprost, że zabiezpieczenie to musi bazować na danych opartych na zdjęciu lub danych biometrycznych.Odnośnie do wydawania dokumentów podróży, paszportów czy dowodów osobistych, też jest już odpowiedni przepis w przepisach prawa. Jeśli chodzi o dostęp do ściśle strzeżonych pomieszczeń i systemów wymagających wysokiego poziomu bezpieczeństwa, to należy zdefiniować, że musi to być wysoki poziom bezpieczeństwa. Powinien być przepis prawa, który mówi, że musimy stosować wysokie środki bezpieczeństwa w odniesieniu do owych systemów. W związku z tym w każdym przypadku powinno się stosować ocenę skutków dla ochrony danych. Chodzi uwzględnienie wszystkich tych elementów – zarówno pozytywnych, jak i negatywnych cech systemu biometrycznego, obaw użytkowników oraz korzyści dla administratora danych. W tym ostatnim przypadku inna będzie sytuacja dla podmiotów publicznych, które z mocy prawa zobligowane są do przetwarzania tylko tych kategorii danych, które są określone w przepisach. Tu musi to zostać określone w przepisie. Inna będzie z kolei ocena dla podmiotów prywatnych. Tu musi być ocena skutków oparta na analizie wymagań dotyczących bezpieczeństwa. Musi również zostać przeprowadzona dokładna analiza skutków dla ochrony prywatności z uwzględnieniem wszystkich stron – w odniesieniu np. do banku i to zarówno jako instytucji, jak i pracownika banku, czyli osoby dokonującej weryfikacji, a także użytkownika, który się jej poddaje.

Na tym chciałbym zakończyć. Dziękuję bardzo.

Przewodniczący poseł Paweł Arndt (PO):

Bardzo dziękuję za tę szczegółową informację. Proszę teraz o zabranie głosu pana ministra Marka Zagórskiego, sekretarza stanu w Ministerstwie Cyfryzacji. Panie ministrze, może troszeczkę krócej niż panowie z GIODO.

Sekretarz stanu w Ministerstwie Cyfryzacji Marek Zagórski:

Ja będę mówił bardzo krótko, panie przewodniczący. Przedstawimy w zespole, bo poproszę za chwilę pana dyrektora Kaweckiego oraz pana profesora Czyżewskiego i pana Sorokowskiego o wspólne przedstawienie naszego punktu widzenia na tę kwestię.

Tytułem wprowadzenia powiem tylko, że odwołując się do sentencji, o której mówił pan radca na samym początku – „bez zuchwałości, bez lęku” – to rozumiem, że pierwsza część była bez zuchwałości, a my teraz spróbujemy trochę bez lęku.

Musimy pamiętać, w jakim kontekście mówimy o danych biometrycznych. Kiedy mówimy o kontekście danych osobowych, to oczywiście włącza nam się światełko ochronne. Ale mówimy o danych biometrycznych dlatego, że one są wykorzystywane nie tylko, bo są wygodne, ale gwarantują w sposób niekiedy najlepszy z możliwych pełną identyfikację osoby. Z punktu widzenia ostatniego elementu, o którym mówił pan dyrektor, czyli środków identyfikacji elektronicznej, oraz tego, że mówimy o poruszaniu się po świecie cyfrowym i mówimy o cyfrowej tożsamości obywateli, to dane biometryczne powinniśmy otoczyć szczególną atencją. I to również dlatego, że dane te, jak każde, mogą

być użyte w niecnych celach. Przede wszystkim jednak mogą gwarantować nam bezpieczeństwo i z tego punktu widzenia także należy spojrzeć na tę kwestię.

Przewodniczący poseł Paweł Arndt (PO):

Bardzo dziękuję, panie ministrze. Rozumiem, że dalsza część...

Sekretarz stanu w MC Marek Zagórski:

Tak, przedstawimy prezentację.

Przewodniczący poseł Paweł Arndt (PO):

Miałbym tylko prośbę, żeby nie powtarzać informacji, które padły już ze strony przedstawicieli GIODO.

Zastępca Dyrektora Departamentu Zarządzania Danymi Ministerstwa Cyfryzacji Maciej Kawecki:

Szanowni państwo, ja też postaram się mówić możliwie krótko i konkretnie.W resorcie cyfryzacji, stojąc przed wyzwaniem przeprowadzenia reformy ochrony danych osobowych i wdrożenia unijnego rozporządzenia do polskiej przestrzeni prawnej, od samego początku stanęliśmy przed założeniem zasady złotego środka. Proszę państwa, trzeba dodać, że to największa reforma, jaka kiedykolwiek była w Polsce przeprowadzana, wymagająca zmiany prawie wszystkich aktów prawnych.

Z jednej strony chronimy prawo podstawowe, jakim bez wątpienia jest ochrona danych osobowych, z drugiej – musimy chronić inne prawo podstawowe, jakim jest swoboda działalności gospodarczej. Podejmowanie decyzji o zaprojektowaniu jakichkolwiek regulacji prawnych zawsze podejmowane jest na podstawie tego właśnie klucza. Klucz ten jest również podstawą do podjęcia decyzji co do budowania, bądź nie, konstrukcji prawnych, które legalizują w przepisach prawnych gromadzenie danych biometrycznych.

Proszę państwa, tutaj w gmachu Sejmu trochę praktyki. Trzeba sobie powiedzieć jasno, że gromadzenie danych biometrycznych jest zabiegiem powszechnym. Gwarantuję państwu, że każda zgromadzona na sali osoba przynajmniej raz udostępniła dziś swoje dane biometryczne. Korzystamy z usług odbioru przesyłek kurierskich i podpisujemy się na elektronicznych nośnikach, oddając swój charakter pisma. Charakter pisma to jedna z najdalej idących danych biometrycznych, ponieważ wskazujących na nasz nastrój w danej chwili, nasz charakter, emocje i to niezależnie od treści, którą nasz charakter pisma odzwierciedla. Korzystają państwo z domofonów we wspólnotach mieszkaniowych, oddając swój głos. Głos to dane biometryczne. Idą państwo do banku i chcą dokonać polecenia przelewu. Co robi pracownik banku? Pierwszą rzeczą, jaką robi, jest zestawienie podpisu na poleceniu przelewu z podpisem, jaki bank ma w systemie teleinformatycznym. To nic innego jak gromadzenie danych biometrycznych. Logują się państwo do telefonów, nie będę mówił marki. Logują się państwo do powszechnie używanych urządzeń, telefonów, wykorzystując linie papilarne, a zatem również dane biometryczne.

Dlaczego ja to wszystko mówię? Dlatego, że powszechne dzisiaj wykorzystanie danych biometrycznych musi być podstawą do podejmowania decyzji na etapie projektodawcy, a później na etapie legislacyjnym co do zalegalizowania podejmowania takich działań na pewnych obszarach, oczywiście wyselekcjonowanych i takich, w których jest to konieczne.

W resorcie cyfryzacji wśród takich obszarów znajduje się na pewno Kodeks pracy i prawo bankowe – jest to jedyny ze wszystkich obszarów działalności gospodarczej, w którym przedsiębiorcy działają, wyłącznie opierając się na środkach wpłaconych przez klientów.

Oczywiście nie jest tak, że resort cyfryzacji nie widzi potrzeby ochrony danych biometrycznych. Widzi taką potrzebę i w związku z tym każda z takich norm prawnych obudowana będzie pewnymi gwarancjami, uprawnieniem do wydawania przez ministra właściwego ds. informacji delegacji rozporządzenia wskazującego, że dane biometryczne gromadzone są w postaci kodu cyfrowego, który gwarantuje, że nawet jego wyciek, bez algorytmu, bez matrycy znajdującej się po stronie administratora, wyłącza możliwość identyfikacji danego użytkownika.

Chciałbym już oddać głos naszym ekspertom, więc na zakończenie chciałbym powiedzieć, że nie bez powodu Unia Europejska po raz pierwszy zdecydowała się na zunifikowanie zasad przetwarzania danych biometrycznych. Dzisiaj dane biometryczne nawet jednym słowem nie są wspominane w ustawie o ochronie danych osobowych, w polskiej legislacji nie występują prawie nigdzie, z wyjątkiem gromadzenia danych biometrycznych w dowodach osobistych. Jednocześnie są powszechnie wykorzystywane. Wydaje mi się więc, że zgodzimy się z Generalnym Inspektorem Ochrony Danych Osobowych w tym obszarze, że doczekaliśmy już takiego czasu, że projektodawca, a potem ustawodawca powinni wypowiedzieć się na temat przetwarzania danych biometrycznych w pewnych obszarach. Dziękuję.

Przewodniczący poseł Paweł Arndt (PO):

Bardzo dziękuję. Rozumiem, że głos zabiorą jeszcze eksperci, tak? Bardzo proszę. Proszę też o przedstawienie się.

Ekspert zewnętrzny Ministerstwa Cyfryzacji prof. Andzej Czyżewski:

Bardzo dziękuję, nazywam się Andrzej Czyżewski, jestem inżynierem z Politechniki Gdańskiem, z tytułem profesorskim.

Poproszę o slajd „Obszary zastosowań biometrii”. Chciałbym powiedzieć, że na co dzień konstruujemy systemy biometryczne i zastanawiamy się nad konsekwencjami,a przede wszystkim nad zabezpieczeniami. Technologia zabezpieczeń bardzo się dziś rozwija. Są zabezpieczenia, są ataki. W cyberprzestrzeni toczy się prawdziwa walka. Dlatego też wszystkie troski Generalnego Inspektora Ochrony Danych Osobowych towarzyszą nam w rozwiązaniach oraz naszym zastanawianiu się na tym, jak używać biometrii.

Chciałbym powiedzieć o kilku sprawach ogólnych, bo nie przyjechałem tu po, żeby angażować państwa w sprawy inżynierskie. Po pierwsze wydaje mi się, że nie da się zatrzymać wodospadu beretem. To takie amerykańskie powiedzenie. Biometria może być traktowana dwojako. Albo będziemy kontynuowali tę walkę na gruncie biometrii, która jest, jak to się mówi po angielsku, *frontier,* polem walki o nową technologię, albo będziemy czekać, aż firmy azjatyckie i amerykańskie zarzucą nas technologiami, które będą gotowe i będziemy musieli je kupować. A mamy w Polsce w tej chwili przewagę nad Stanami Zjednoczonymi, Zjednoczonym Królestwem i wieloma innymi państwami, jeśli chodzi o tzw. FinTech EngineTech, czyli technologię operacji finansowych i ubezpieczeniowych, bo weszliśmy późno i mamy profit przewagi wejścia w najwyższą technologię.

Uważam, że w dziedzinie biometrii mamy w tej chwili naprawdę sporo do powiedzenia. Trzeba tylko podejść do tego nie całościowo, tylko różnicować, czyli zrozumieć, na czym polegają uwarunkowania rozwoju. Slajd w pewien sposób pokazuje konieczność różnicowania. Jeśli chodzi o bankowość i sektor publiczny, to są to instytucje zaufania publicznego. Biometria stanowi tutaj wspaniałe pole zastosowań. W tym temacie możemy się dogadać z GIODO, dlatego że są tam wdrożone bardzo zaawansowane mechanizmy ochrony danych osobowych, które są zabezpieczone od strony prawnej, podlegają audytom itd.

Moglibyśmy wykorzystać rozwój technologii FinTech EngineTech do tego, żebyśmy wykorzystali przewagę technologiczną dla rozwoju biometrii. Jeżeli chodzi o środkową kolumnę, czyli sprzedaż i rozrywkę, to zostawmy to może Amerykanom, którzy się w tym specjalizują, bo chyba ich nie dogonimy. Trzeba byłoby uważać, żeby nie stworzyć mechanizmów przekazywania danych biometrycznych naszych obywateli do światowych sieci. Raz przekazane surowe dane biometryczne w zasadzie są tam już na zawsze. Jeżeli ktoś przekaże swoją tożsamość, np. głos, twarz czy inne tego typu dane, nie będzie ich mógł skasować. Tylko przeszczep twarzy może go uratować przed tym, że ktoś już do końca jego życia będzie to wykorzystywał. Prosiłbym więc o zróżnicowanie podejść od profesjonalnego po rozrykowe, które jest niepotrzebne i nieważne. Zresztą to padało w pańskim wystąpieniu o celowości. Ja to tylko w ten sposób potwierdzam.

Jeżeli chodzi o prawą kolumnę, czyli operacje mobilne i kontrole dostępu, to są to dwie różne sprawy. Operacje mobilne sa niezwykle wrażliwe na atak i to nie tylko dlatego, że tak się nam może wydawać, że bajty latają w powietrzu i ktoś może się włamać, bo tak nie jest. Transmisja jest naprawdę zabezpieczona i nieważne, czy odbywa się po kablu czy drogą bezprzewodową. Natomiast pewne technologie biometryczne są niezwykle

wrażliwe na atak. Powiedzmy np. o autentykacji głosowej, nagrawaniu czyjegoś głosu. Naiwne technologie ataku były takie, że można było nagrać czyjść głos i się włamać. Dziś mamy do czynienia z biometrią interaktywną, czyli klient transakcji finansowej musi odczytać unikatowy komunikat, który pojawia mu się na monitorze. Ale i z tym sobie poradzono, bo wykonuje się tzw. syntezę mowy.W technologiach mobilnych mamy niestety słabszą kontrolę nad tym, co się dzieje po drugiej stronie, i jest to jak gdyby inny rozdział, który wymaga szczególnej uwagi.

Jeśli chodzi o kontrolę dostępu, to natrafia ona z kolei na prawo pracy. Do czego można zmusić pracownika, żeby przyszedł i wykonał swoją pracę? Czy musi się on identyfikować, przykładać rękę i specjalnie się identyfikować?

Poproszę następny slajd. Może pan zechce skomentować? Pan z firmy...

Ekspert zewnętrzny Ministerstwa Cyfryzacji Jerzy Sorokowski:

Jerzy Sorokowski, ekspert z firmy Fujitsu. Jesteśmy producentem jednej z technologii biometrycznych. Chciałbym się odnieść do poprzedniego slajdu, ponieważ zabrakło mi tam jednego ważnego punktu; mianowicie ochrony zdrowia.

Kiedy mówimy o zastosowaniach biometrii, nie można pominąć zastosowań, które są tam stosowane, z bardzo prostego powodu. W wypowiedzi GIODO pojawiło się stwierdzenie o proporcjonalności użycia lub adekwatności co do celów. Otóż ochrona zdrowia jest idealnym przykładem, że adekwatność użycia może być argumentem za stosowaniem biometrii.

Na całym świecie, również w Polsce, wdrażany jest obecnie tzw. elektroniczny wers w danych medycznych, który umożliwia dostęp wszystkim jednostkom medycznym do wspólnych danych medycznych pacjenta. Wbrew pozorom rodzi to bardzo poważny problem z ochroną danych osobowych lub danych wrażliwych, które znajdują się w tego typu systemie. W tej chwili w Stanach Zjednoczonych coraz częściej technologię biometryczną wykorzystuje się do tego, żeby kontrolować dostęp do tych danych. Tak naprawdę biometria stoi więc na straży poufności danych wrażliwych pacjenta. To jedno zastosowanie.

Było też tutaj wspominane, że technologię tę stosuje się do identyfikacji pacjentów. Rzeczywiście w Stanach Zjednoczonych jest to coraz bardziej powszechne. Są stosowane przenośne zestawy do pomiarów biometrycznych, które są wykorzystywane w przypadkach takich, jak nieprzytomne dziecko, dziecko w szoku pourazowym, z którym nie można nawiązać kontaktu. To samo dotyczy osób dorosłych. Jest to bardzo istotna sprawa, żeby podjąć adekwatne leczenie, które nie zaszkodzi pacjentowi. Jak widać, biometria nie jest tylko łatwością identyfikacji pacjenta, ale także ochroną jego zdrowia lub nawet życia.

Jeśli chodzi o inne przykłady, to mamy tutaj zastosowanie ze szpitali psychiatrycznych, np. w Anglii czy Stanach Zjednoczonych, które wykorzystują technologię biometryczną właśnie po to, żeby chronić zdrowie i życie pacjentów.

Ekspert zewnętrzny MC prof. Andrzej Czyżewski:

Proszę państwa, wyobraźmy sobie, że potrzebujemy dzisiaj pamiętać różne hasła dostępu do bardzo wielu systemów cyfrowych. Potrzebujemy jakichś dokumentów mniej lub bardziej biometrycznych, potrzebujemy kart. Wyobraźmy sobie przyszłość, czyli następną rewolucję technologiczną, która będzie tak silną rewolucją, jaką były komputery osobiste i internet. Ktoś rodzi się, jest wyposażony przez matkę naturę w cechy biometryczne i dzięki temu może właściwie przez całe życie podążać tam, gdzie został zweryfikowany. Chodzi mi tutaj o dostęp do różnych usług, serwisów, korzystanie z linii lotniczych itd. A to wszystko tylko dlatego, że jest sobą, posiada taki, a nie inny kształt twarzy, tembr głosu, różne cechy biometryczne typu tęczówka, siatkówka itd.

Technologia dorośnie do tego. Dzisiaj dopiero burzliwie się rozwija. Ciekawe są wyniki badań opinii publicznej na ten temat. Otóż już na dzień dzisiejszy 49% populacji, to jest ślepa próba, czyli dotyczy ludzi niemających za wielkiego pojęcia technicznego o biometrii, chciałoby się pozbyć wszelkich dowodów tożsamości i być weryfikowanymi biometrycznie. Wyobrażam sobie, co się stanie w najbliższych latach, kiedy te technologie się rozwiną i staną się równie przyjazne co telefony komórkowe. Tutaj pokazany jest

pewien podział. Najszybciej ludzie chcieliby zmian w bankomatach – po prostu zbliżyć się i wypłacić pożądaną kwotę – ale również innych tak zwanych modalności.

W tym miejscu wspomnę o tzw. biometrii multimodalnej. Do dzisiaj nie za bardzo znaleziono technologię, która byłaby jedynie słuszna, ale to, co odbywa się w tej chwili na zapleczach technologicznych wielkich firm na świecie, to połączenie ze sobą kilku modalności biometrycznych, czyli rzeczywiście tak jak my rozpoznajemy człowieka. Jak państwo przyjdą do banku i wasz doradca bankowy was zna, to bierze on pod uwagę kilka cech biometrycznych, żeby was rozpoznać wizerunek, kształt twarzy, sposób zachowania się, głos itd. To jest to, do czego w tej chwili dążą rozwiązania technologiczne. Nie jedyne słuszne rozwiązanie, które jest dyskusyjne, ale kilka jednocześnie.

Będę już kończył, żeby państwa nie zanudzać. O skuteczności biometrii decyduje jej unikatowość, trwałość, uniwersalność i bezpieczeństwo. Chciałbym podkreślić to, co mówił pan ekspert z GIODO. Mianowicie wszyscy, którzy pracują nad biometrią, unikają przekazywania danych surowych. Powiedziałem już wcześniej, że zapisanie danych surowych jest dla każdego bardzo niebezpieczne. To jesteśmy my, tam są wszystkie nasze dane, których nie możemy zmienić do końca życia. Z naturalnej świadomości inżynierskiej nikt nie przekazuje tego typu danych do systemu baz. Wszyscy kodują te dane, wyciągają z nich pewne cechy do ropoznawania, czy to układu żył, o czym pewnie jeszcze powie pan Sorokowski, czy to pewnych cech pomiarowych twarzy, czy pewnych cech brzmienia głosu. Zatem należałoby się skupić na przeciwdziałaniu temu, żeby ktokolwiek pobierał nasze surowe dane biometryczne i je zapisywał. Natomiast, jeżeli chodzi o zapisywanie wyciągniętych z danych biometrycznych cech, to musimy to dopuścić, bo jak nie, to zrobi to za nas technologia.

Poproszę o ostatni slajd, który chciałbym omówić.Wracajac do multimodalności, gdybyśmy znaleźli w tabelce jeden wiersz, który jest cały na zielono, to bylibyśmy szczęśliwi. Chodzi o to, że jeżeli bezpieczeństwo i praktyczność weryfikacji biometrycznej byłaby idealna, to pewnie jedna technologia by zwyciężyła. Natomiast, jeżeli przychodzimy do banku i ktoś nam reklamuje technologię skanowania naszej tęczówki, to mówimy do opiekuna: proszę pani/pana, nie przyszliśmy tutaj do okulisty, nie będziemy przykładać oka, nie będziemy wkładać palca w jakiś otworek, bo nie wiemy, czy go wyjmiemy, czy nie pobiorą nam krwi. Wygoda biometrii jest więc sprawą absolutnie zasadniczą. Kompromisem, który może być osiągnięty, jest stosowanie biometrii wielomodalnej. Proszę mi wierzyć, bo znam jawne i mniej jawne wyniki badań, które odbywają się na świecie. Jesteśmy absolutnie w przededniu rewolucji biometrycznej. Na ile my jako kraj będziemy w tym uczestniczyli, to zależy wyłącznie od nas. Dziękuję.

Sekretarz stanu w MC Marek Zagórski:

Panie przewodniczący, to tyle z naszej strony. Chciałbym tylko podkreślić, że nalegaliśmy na uzupełnienie prezentacji Generalnego Inspektora Ochrony Danych Osobowych po to, aby w kontekście zbliżających się prac nad ustawą, które trafią zapewne także do Wysokiej Komisji, pogląd na tę kwestię był bardziej zrównoważony. Dziękujemy za przychylenie się do naszej prośby.

Przewodniczący poseł Paweł Arndt (PO):

Ja również dziękuję za tę prezentację i wszystkie szczegóły, które usłyszeliśmy. Nasza Komisja ma w tytule innowacyjność. Nie ma więc żadnych wątpliwości, że biometria to dziedzina przyszłości, dziedzina innowacyjna i chyba coraz częściej będziemy o niej mówili.

Otwieram dyskusję. Kto z państwa posłów chciałby zabrać głos? Pan poseł Arkadiusz Marchewka.

Poseł Arkadiusz Marchewka (PO):

Dziękuję, panie przewodniczący. Panie ministrze, szanowni państwo, rozmawiamy o przyszłości. To wręcz pasjonujące, jak możemy wykorzystywać takie możliwości w codziennym życiu, jak sprawdzenie naszej tożsamości może ułatwić nam życie w wielu sprawach, chociażby w przysłowiowym pójściu na siłownię.

Nie będę pytał o szczegóły funkcjonowania biometrii, bo zostało to w bardzo dobry i klarowny sposób przedstawione, natomiast interesuje mnie kwestia spojrzenia w przy-

szłość w kontekście tego, jak będziemy w Polsce wdrażać takie działania. Niedawno przedstawiona została koncepcja nowego e-dowodu, który ma zacząć być wydawany w pierwszym kwartale 2019 r. Myślę, że do tego czasu przepisy, o których panowie mówiliście, wejdą w życie.

Jeśli dobrze odczytuję to, co jest napisane w koncepcji tego dokumentu, to będzie on zawierał aplikację, która w swojej warstwie elektronicznej będzie mogła przechowywać dane biometryczne. Czy dobrze to odczytuję? Jeśli tak, to chodzi o to, żeby w różnych miejscach użyteczności publicznej przykładać dowód, wpisywać PIN i się weryfikować. Skoro już patrzymy w przyszłość i będziemy dążyć do wyposażenia jak największej liczby polskich instytucji publicznych i podmiotów prywatnych w narzędzia do weryfikacji, to może warto popatrzeć dwa kroki dalej i zastanowić się nad kwestią biometrii? Skoro takie cechy będziemy i tak zostawiać w rejestrach państwowych, to może warto, aby były one możliwe do zapisania w warstwie elektronicznej dowodu. To jest tylko takie wybiegnięcie w przyszłość. Nie wiem, czy na tym etapie rozmawianie o tym jest w ogóle możliwe. Koncepcja, o której wspomniałem, to dopiero przyszłość. Rozpoczyna się dopiero za dwa lata, a kończy po praktycznie10 latach. Skoro jednak te rozwiązania pojawiają się na horyzoncie, to może warto wsiadać do pociągu, który rusza, zamiast stać na peronie. Dziękuję.

Przewodniczący poseł Paweł Arndt (PO):

Bardzo dziękuję panu posłowi.

Sprawa, o której mówimy, jest rzeczywiście niezwykle ważna, ciekawa i przyszłościowa. Panowie mówili, żebyśmy podchodzili do tego bez bojaźni. Nie wiem, czy to zawsze będzie możliwe. Sami przekazywaliście panowie dane, które nakazują nam jednak pewną ostrożność w podchodzeniu do biometrii. Zanim pan minister czy panowie odpowiedzą na pytania czy wątpliwości pana posła Marchewki, chciałbym zapytać, czy nasi goście chcieliby zabrać głos? Mamy przedstawicieli MSWiA, policji, a więc osoby, które w jakiejś mierze interesują się, zajmują się sprawą i mogą przekazać nam interesujące dane.

Czy ktoś z państwa chciałby zabrać głos? Nie ma specjalnie chętnych. Panie ministrze, gdyby zechciał się pan odnieść do tych wypowiedzi...

Jest jednak jakiś głos. Bardzo proszę o przedstawienie się.

Zastępca Dyrektora Departamentu Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji Mariusz Cichomski:

Mariusz Cichomski, zastępca dyrektora Departamentu Porządku Publicznego MSWiA. Właściwie chciałem się tylko wpisać w wypowiedź przedstawicieli pana ministra i przedstawicieli Ministerstwa Cyfryzacji, bo my też stoimy przed bardzo dużym wyzwaniem natury prawnej w odniesieniu do danych osobowych. Mianowicie wdrożenia rozwiązań związanych z dyrektywą policyjną, o której była mowa na jednym z wcześniejszych posiedzeń Wysokiej Komisji.

Mamy te same terminy, te same wyzwania, rozpoczynamy współpracę. Miejmy nadzieję, że jak najszybciej i jak najlepiej uda nam się stworzyć wspólne mechanizmy, wspólną płaszczyznę ochrony danych osobowych z uwzględnieniem tych wymogów, które organy ścigania, szeroko rozumiane, bo dyrektywa policyjna obejmuje dużo więcej niż służby ministra właściwego ds.wewnętrznych czy chociażby służby specjalne w pewnym zakresie, poza elementami bezpieczeństwa narodowego... To jest też element, który na pewno będziemy dyskutować na poziomie tej Komisji. Zwracamy na to uwagę jako na jedno z największych wyzwań legislacyjnych z punktu widzenia Ministerstwa Spraw Wewnętrznych i Administracji...

Przewodniczący poseł Paweł Arndt (PO):

Bardzo dziękuję. Panie ministrze, bardzo proszę.

Sekretarz stanu w MC Marek Zagórski:

Nie chcę już wracać do historii, że jesteśmy opóźnieni z e-dowodem o ileś lat. To też jest przyczyna, że możemy jeszcze dzisiaj dyskutować o innym jego zastosowaniu. Odpowiedź na pytanie, dlaczego nie możemy zrobić jeszcze kroku, o którym pan poseł mówi,

jest zawarta w wyświetlanym własnie slajdzie. Nie mamy jeszcze takiej technologii, która byłaby pewna, uniwersalna.

Poseł Arkadiusz Marchewka (PO):

W kontekście bezpieczeństwa?

Sekretarz stanu w MC Marek Zagórski:

W kontekście bezpieczeństwa, popularności i akceptowalności takiego rozwiązania. Pamiętajmy też, że mówimy o dowodzie osobistym i o 49% osób, które chcą korzystać z biometrii, ale to jeszcze wciąż tylko 49%.

Powiem inaczej i proszę to traktować nie jako stanowisko rządu, a element dyskusji dwóch posłów. Być może środki identyfikacji elektronicznej rozwiążą ten problem, być może plastikowy dowód nawet z warstwą elektroniczną, o którym mówimy, to ostatnie podejście do takiego rozwiązania, a środki identyfikacji elektronicznej, bazujące także na biometrii rozwiążą nasz problem. Myślę, że jest to kwestia, jak mówił pan profesor, może 2-3 lat. Wtedy kiedy jakaś technologia weźmie górę, będziemy mogli powiedzieć, że tak, mamy to już rozwiązane. Dzisiaj jesteśmy w takim miejscu, w jakim jesteśmy. Pomijając wszystkie inne kwestie, dopiero 50% społeczeństwa jest w stanie akceptować takie rozwiązania. To też musimy brać pod uwagę. Dziękuję bardzo.

Przewodniczący poseł Paweł Arndt (PO):

Dziękuję bardzo. Pan Paweł Makowski chciał jeszcze zabrać głos.

Radca w Biurze GIODO Paweł Makowski:

Ja bardzo krótko w kontekście podniesionej przez pana posła kwestii, czyli przyszłych prac legislacyjnych związanych z wdrażaniem jakichś technologii.

Chciałbym tylko zwrócić uwagę na jeden bardzo ważny przepis ogólnego rozporządzenia, które będziemy stosować bezpośrednio. Chodzi o art. 35 ust. 10 tego rozporządzenia, który mówi o tym, że wszędzie tam, gdzie projektuje się nowe rozwiązania legislacyjne, należy w trakcie dokonywania oceny skutków regulacji dokonać oceny skutków dla ochrony danych. Chodzi o to, że na etapie projektowania jakiegoś aktu prawnego czy rozwiązania trzeba zastanawiać się, jaki może mieć ono wpływ na prywatność, jakie ryzyko dla prywatności niesie – tak żeby wybrać jak najlepsze rozwiązanie. Myślę, że to będzie bardzo duże wyzwanie dla wszystkich legislatorów, którzy zajmują się w naszym kraju tworzeniem prawa, żeby ocenę skutków ochrony danych wbudowywać w mechanizmy OSR.

Jeszcze tylko jedna rzecz, dotycząca harmonizacji działań w kontekście wdrożenia RODO i implementacji dyrektywy, która będzie regulować przetwarzanie danych w sektorze wymiary sprawiedliwości i organów ścigania. Z naszej perspektywy jest to niesłychanie ważne. Pamiętajmy, że reforma prawa ochrony danych osobowych została wprowadzona pakietem, czyli ogólne rozporządzenie i dyrektywa zawierają bardzo wiele tych samych elementów czy instumentów prawnych. To niesłychanie ważne, żeby te dwa resorty odpowiedzialne za dostowanie polskiego prawa do reformy robiły to w sposób zharmonizowany. Bardzo dziękuję.

Przewodniczący poseł Paweł Arndt (PO):

Bardzo dziękuję. Czy jeszcze ktoś z państwa chciałby zabrać głos?

Jeśli nie, to chyba mogę stwierdzić, że wyczerpaliśmy porządek obrad. Dziękuję za ciekawą dyskusję. Wszystko jeszcze przed nami, duże wyzwania i myślę, że tak jak powiedział pan profesor, nikt beretem wodospadu nie będzie zatrzymywać.

Dziękuję bardzo. Stwierdzam zakończenie posiedzenia Komisji. Protokół z posiedzenia z załączonym zapisem jego przebiegu będzie do wglądu w sekretariacie Komisji w Kancelarii Sejmu. Bardzo dziękuję.